

JUDGE ROBERT J. BRYAN

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA,)	No. CR15-5351RJB
)	
Plaintiff,)	MOTION AND MEMORANDUM OF
)	LAW IN SUPPORT OF MOTION TO
v.)	DISMISS INDICTMENT
)	
JAY MICHAUD,)	Noted: December 4, 2015
)	
Defendant.)	<i>[Evidentiary Hearing Requested]</i>

I. INTRODUCTION

Jay Michaud, by his attorneys Colin Fieman and Linda Sullivan, respectfully moves the Court pursuant to Fed. R. Crim. R. 12(a)(3) and the Court's supervisory powers for an order dismissing the indictment in this case, with prejudice, based on outrageous government conduct. This motion arises from the Government's operation of a massive child pornography site and its widespread distribution of child pornography between February 20, 2015, and March 4, 2015, as part of the investigation leading to the charges against Mr. Michaud. The unprecedented nature and scope of the Government's distribution of contraband in connection with this case has no legal justification or excuse and offends commons standards of decency. Accordingly, the Court can and should dismiss the indictment in this case.

II. STATEMENT OF FACTS

As the Court is aware from earlier pleadings, the Government took direct and exclusive control of “Website A” on February 20, 2015, and continued to maintain and operate the site until at least March 4, 2015. *See, e.g.*, Exh. A at 4 (complaint in related NIT case *United States v. Bingham*, 15MJ-318DBP (D. Utah Sept. 23, 2015)); Motion to Suppress, exh. C at ¶ 30 (Dkt. 29) (the FBI took “administrative control” of “Website A” and relocated the server to a “government-controlled” location). During this time, the site had over 214,000 members, 117,000 postings, and an untold number of illicit pictures, videos, and links to additional illegal content. *See, e.g.*, exh A at 4. The defense has served the Government with supplemental discovery demands for, *inter alia*, the exact number of visitors to the site while the FBI was running it; the number of pictures and videos that the FBI maintained and added to the site during that time; and the number of pictures and videos that were downloaded by users during the same period.¹ While the Government has declined to disclose this information, it has described the site as “the largest remaining known child pornography hidden service in the world.” *Id.* at 4.

More specifically, it appears that “Website A” did not explicitly promote itself as a child pornography site (for example, it is not obvious from the home page that it contains illegal images). *See* exh. B (filed under seal) (screen shot of the home page as it appeared on February 20, 2015). In addition, the site was divided between subdirectories and forums that did not contain child pornography (including “fiction,” “artwork,” and chat sections), as well as other sections that were obviously geared

¹ On October 22, 2015, the defense served the Government with supplemental discovery demands for, *inter alia*, the items described above in the text. The Government’s refusal to provide this and other discovery is the subject of the defense’s accompanying motion to compel discovery.

1 toward the posting and distribution of child pornography. However, based on the
2 available discovery and the Government's characterizations of the site's content, it is
3 apparent that the illicit subdirectories and forums contained many thousands of pictures,
4 videos and links to child pornography. The Government has also disclosed that an
5 average of 11,000 unique visitors accessed the site each week (*i.e.* visits by individual
6 users, without counting repeat visits by the same users), many of whom posted,
7 downloaded and redistributed child pornography while on the site.

8 Further, the Government has confirmed that during its control and operation of
9 the site it took no steps to limit or impede the downloading or redistribution of the site's
10 illegal content. Although, as discussed below, there are available technical means that
11 would have allowed the FBI to deploy its "Network Investigative Technique" (NIT)
12 against users who tried to access illegal content on the site without distributing the
13 actual content to them, the Government has confirmed that it elected to distribute child
14 pornography during the entire time it was operating the site.

15 **III. ARGUMENT**

16 **THE GOVERNMENT'S OPERATION OF THE WORLD'S LARGEST** 17 **"HIDDEN SERVER" CHILD PORNOGRAPHY SITE AND ITS GLOBAL** 18 **DISTRIBUTION OF UNTOLD NUMBERS OF PICTURES AND VIDEOS** 19 **IS OUTRAGEOUS CONDUCT THAT SHOULD RESULT IN** 20 **DISMISSAL OF THE INDICTMENT.**

21 The remedy the defense is seeking is extraordinary, but only because the
22 Government's conduct in this case appears to be unprecedented and would appall the
23 average citizen. Criminal investigations should seek to contain and mitigate the harm
24 caused by illegal activity, not perpetuate that harm and (according to the Government's
25 own oft-repeated statements) "re-victimize" the children depicted in the images that it
26 distributed.

1 The Supreme Court has long stated that “[r]egard for the requirements of the
 2 Due Process Clause ‘inescapably imposes upon this Court an exercise of judgment
 3 upon the whole course of the proceedings (resulting in a conviction) in order to
 4 ascertain whether they offend those canons of decency and fairness which express the
 5 notions of justice of English-speaking peoples even toward those charged with the most
 6 heinous offenses.’” *Rochin v. California*, 342 U.S. 165, 169 (1952) (quoting *Malinski v.*
 7 *People of State of New York*, 324 U.S. 401, 416-17 (1945)). The Court went on to
 8 explain that “[t]hese standards of justice are not authoritatively formulated anywhere as
 9 though they were specifics. Due process of law is a summarized constitutional
 10 guarantee of respect for those personal immunities which, as Mr. Justice Cardozo twice
 11 wrote for the Court, are ‘so rooted in the traditions and conscience of our people as to
 12 be ranked as fundamental’ or are ‘implicit in the concept of ordered liberty.’” *Id.*
 13 (citations omitted).

14 Government conduct that is so outrageous that it offends our shared canons of
 15 fairness and decency to a degree warranting dismissal of an indictment is rare, and the
 16 standard for dismissal on this ground is “extremely high.” *United States v. Smith*, 924
 17 F.2d 889, 897 (9th Cir. 1991). Specifically, an indictment can be dismissed only where
 18 the Government’s conduct is “so grossly shocking and so outrageous as to violate the
 19 universal sense of justice.” *United States v. Stinson*, 647 F.3d 1196, 1209 (9th Cir.
 20 2011) (quoting *United States v. Restrepo*, 930 F.2d 705, 712 (9th Cir. 1991)); *accord*,
 21 *United States v. Pedrin*, 797 F.3d 792, 795–96 (9th Cir. 2015) (quoting *Stinson*). When
 22 governmental misconduct involves “nonconstitutional error,” courts should not dismiss
 23 an indictment unless the misconduct resulted in “fundamental” errors that had a
 24 “substantial influence” on the outcome of the case. *Bank of Nova Scotia v. United*
 25 *States*, 487 U.S. 250, 256 (1988). In addition, in cases involving misconduct that

1 results in “an error of constitutional magnitude,” courts should also first determine
2 whether other remedies are available or whether they are “impractical.” *Id.* at 257.

3 In this case, the Court should find that the Government’s misconduct during the
4 investigation of this case, which appears to be unprecedented, warrants dismissal of the
5 indictment. While another and more routine potential remedy has been presented to the
6 Court through Mr. Michaud’s motion to suppress, an order of suppression may not
7 adequately convey the level of disapprobation with which the Government’s actions
8 should be met.² The Court need only consider some of the Government’s own
9 pronouncements about the harm caused by the proliferation of child pornography to
10 fully realize how troubling the Government’s “Website A” operation is. While the
11 defense does not necessarily agree with some of the Government’s more extreme
12 statements about the impact of downloading or distributing illicit pictures, it is
13 impossible to reconcile the Government’s operation of “Website A” with its own view
14 of the harm caused by the proliferation of child pornography.

15 For example, the Department of Justice’s web site states the following:

16 [V]ictims of child pornography suffer not just from the sexual abuse inflicted
17 upon them to produce child pornography, but also from knowing that their
18 images can be traded and viewed by others worldwide. Once an image is on the
19 Internet, it is irretrievable and can continue to circulate forever. The permanent
20 record of a child’s sexual abuse can alter his or her live (*sic*) forever. Many
21 victims of child pornography suffer from feelings of helplessness, fear,
humiliation, and lack of control given that their images are available for others to
view in perpetuity.³

22 ² The defense is preparing and will soon file a Second Motion to Suppress and Motion
23 for *Franks* Hearing, which will allege additional Fourth Amendment violations in support of an
24 order of suppression.

25 ³ Available at: <http://www.justice.gov/criminal-ceos/child-pornography>. This statement
26 appears as part of the mission statement for the Child Exploitation and Obscenity Section
(CEOS), which apparently approved and supervised the “Website A” operation.

DOJ also routinely emphasizes in its press releases that possessing and circulating pornographic images re-victimizes the children depicted in them. *See, e.g.,* DOJ Press Release, *Ellettsville Man Charged with Production of Child Pornography*, April 15, 2015 (“Producing and distributing child pornography re-victimizes our children every time it is passed from one person to another”).⁴ Indeed, the Government has expressed the view that even looking at an image of child pornography re-victimizes children. *See, e.g.,* FBI.gov, *Defendant Sentenced for Possession of Child Pornography*, November 5, 2013 (justifying a 108 month sentence for a U.S. Air Force airman who possessed child pornography on the ground that “he caused the young children in these disgusting images to be re-victimized every time he looked at the pictures.”).⁵

The harm caused by simply possessing, let alone distributing, illegal pictures is one that is also routinely emphasized in the Government’s sentencing memos. For example, in a recent sentencing memo for a defendant convicted of distribution, the Government explained its views as follows:

The distribution and possession of child pornography – images and videos of real children experiencing the worst moments of their lives – is not a “victimless” crime, and the heinous nature of these offenses should never be diminished by referring to them as “just pictures.” These are crime scene photographs of children being raped. The children portrayed in the videos and images. . . suffer real, permanent, and lifelong damage. Not only do these

⁴ Available at: <http://www.justice.gov/usao-sdin/pr/ellettsville-man-charged-production-child-pornography>.

⁵ Available at: <https://www.fbi.gov/atlanta/press-releases/2013/defendant-sentenced-for-possession-of-child-pornography>. It should be noted here that several studies have determined that most child pornography possession and distribution offenders have no history of molesting minors and pose no significant future risk of doing so in the future. *See, e.g.,* Endrass et al, *The Consumption of Internet Child Pornography and Violent Sex Offending*, BMC Psychiatry (2009).

1 children suffer physically at the hands of their rapists and molesters, *they suffer*
2 *emotionally each and every time their exploitation is shared over the Internet.*

3 *United States v. Corbitt*, CR12-5289RBL, Dkt. 84 (Government Sentencing Memo) at 7
4 (emphasis added); *see also, e.g.*, CR13-5028RJB, Dkt. 48 (Government Sentencing
5 Memo) at 6 (“Every participant in the chain – producer, distributor, consumer –
6 sustains the market for these images, and each victim, whether identified or not, suffers
7 not only when an image is created, but each and every time an image is viewed”).

8 Lest the Government miss the point of highlighting these statements, the issue
9 here is not whether the possession or distribution of child pornography has harmful
10 effects, or whether the children who were abused in the making of such horrible images
11 are deserving of the utmost sympathy and care. The issue instead is how, while
12 decrying the long-term and widespread consequences to those portrayed of even
13 someone viewing illicit images, the Government can possibly justify the massive
14 distribution of child pornography that it accomplished in this case.

15 Certainly, it is no answer that the FBI did this as part of an effort to apprehend
16 people who view or download child pornography. Setting aside the dubious morality of
17 asserting that the investigative ends justify such outrageous means, the fact is that there
18 are other ways of targeting users who wanted to access illegal content on the site
19 without the Government actually distributing it. For example, in other investigations,
20 the FBI has monitored child pornography sites and posted links to pictures or videos
21 with explicit titles. When a visitor to the forum clicked on a link, an NIT would capture
22 IP information, but the link itself was blocked or an “error” message would appear.
23 Alternatively, investigators can use a “spoofing” system, where visitors to a target site
24 are secretly redirected to a server with a facsimile of the site, minus any content or links
25 that investigators do not want to remain accessible or downloadable. In this case, by
26

1 contrast, the FBI not only obtained a warrant that allowed it to target anyone who
 2 visited “Website A’s” home page (even though it is not obviously a child pornography
 3 site and much of its content was legal), but it continued to distribute thousands of illicit
 4 pictures and videos to thousands of visitors.

5 No doubt law enforcement agents often use contraband, like drugs or guns, as
 6 part of undercover “buys” or to execute a sting operation. But in such cases responsible
 7 agents make every effort to control, track and recover the contraband they are using. In
 8 this case, what the Government did is comparable to flooding a neighborhood with
 9 heroin in the hope of snaring an assortment of low-level drug users. *Compare also*
 10 DOJ, Office of the Inspector General, *A Review of the ATF’s Operation Fast and*
 11 *Furious and Related Matters* (September, 2012) (criticizing DOJ’s handling of “gun
 12 walk” investigations that resulted in the uncontrolled distribution of numerous
 13 firearms).⁶

14 Online investigations are especially sensitive and problematic because agents
 15 have no ability to control the redistribution of pictures, malware or other contraband
 16 once they are introduced to the Internet. As a result, the Department of Justice itself
 17 cautions its attorneys and agents about the potential harms that can arise from online

18 ⁶ Available at <https://oig.justice.gov/reports/2012/s1209.pdf> . *See also, e.g.,*
 19 <http://democrats.oversight.house.gov/sites/democrats.oversight.house.gov/files/documents/7-26-11-Full-Committee-Hearing-Transcript.pdf> at 18-19 (testimony of ATF Senior Special
 20 Agent Jose Wall) :

21 I was skeptical when the first whistle-blower came to this committee with allegations of
 22 hundreds maybe thousands of guns being allowed to walk into the country of Mexico. I
 23 could not believe that someone in ATF would so callously let firearms wind up in the
 24 hands of criminals, but it appears that I was wrong . . . and that this activity has
 25 seemingly been approved by our own Justice Department and ATF management in the
 26 misguided hope of catching the “big fish.” Having had enough experience with gun
 trafficking investigations, I can only imagine that once the DOJ OIG report was
 released, a report that was critical of ATF efforts in stopping gun trafficking, the
 emphasis changed to following the food chain up to the leaders. What the persons
 approving this debacle failed to realize is that the end does not justify the means.

1 investigations and requires special approval for operating any type of “online
2 undercover facility.” DOJ, *Online Investigative Principles for Federal Law*
3 *Enforcement Agents* (available at: [https://info.publicintelligence.net/DoJ-](https://info.publicintelligence.net/DoJ-OnlineInvestigations.pdf)
4 [OnlineInvestigations.pdf](https://info.publicintelligence.net/DoJ-OnlineInvestigations.pdf)). DOJ’s investigative principles emphasize that law
5 enforcement agencies must consider several novel and sensitive issues when
6 determining whether to approve the establishment of an online undercover facility:

7 First, online undercover facilities that offer the public access to information or
8 computer programs that may be used for illegal or harmful purposes may have
9 greater capacity than similar physical-world undercover entities to cause
10 unintended harm to unknown third parties. *Because digital information can be*
11 *easily copied and communicated, it is difficult to control distribution in an*
12 *online operation and so limit the harm that may arise from the operation.*

13 *Id.* at 44 (p. 57 of the PDF) (emphasis added).

14 The statement of principles goes on to caution that the use of online undercover
15 facilities raises complex legal and policy issues, “especially if law enforcement agents
16 seek to use the system administrator’s powers for criminal investigative purposes.”
17 These include “unique and sensitive policy issues involving privacy, international
18 sovereignty, and unintended harm to unknown third parties.” *Id.* at x (p. 11 of the
19 PDF). Because of these concerns, DOJ requires any investigation involving an online
20 undercover facility to undergo a special review and approval process. *Id.*

21 This document also compares online “sting” operations with other operations
22 employing tools of criminality. Using an example of selling “cloned phones,” DOJ
23 pointed out that law enforcement agents “can prevent or minimize the potential for
24 harm caused by their activities by, for example, arresting targets before they can use the
25 phones or requesting the cellular carrier to block or limit access by these particular
26 phones to the cellular network.” *Id.* at 44 (p. 57 of the PDF). Even when that cannot

1 occur, the harm is constrained by the fact that “a single ‘clone phone’ can only be used
2 by one individual at a time and cannot be duplicated and redistributed to multiple
3 users.” *Id.*

4 Similar limits, however, are difficult to impose on online undercover operations,
5 as DOJ itself cautions in its policy statement:

6 [T]he online facility is likely to be automated, making it difficult for the agents
7 to limit who obtains the tools or the damage that the tools end up causing to
8 innocent third parties. Further, unlike the clone phone, the hacker tools can be
9 *endlessly replicated and distributed to others in a manner that law enforcement
agents cannot easily control.*

10 *Id.* at 45 (p. 58 of PDF) (emphasis added). Unfortunately, in this case, it appears that
11 the FBI failed to take any measures whatsoever to control the replication and
12 distribution of images from its undercover website.

13 Given DOJ’s stated policies and procedures, the defense has asked the
14 Government to disclose all records related to DOJ’s review, approval and supervision
15 of the “Website A” operation. The Government has so far declined to provide these
16 records, and as a result these requests are part of the defense’s accompanying Motion to
17 Compel Discovery. Full disclosure of both the extent of the “Website A” operation
18 (including the number of pictures and videos the FBI distributed while in control of the
19 site) and how it was approved and supervised will allow this Court fully to assess the
20 degree which the Government’s actions offend “those canons of decency and fairness”
21 which inform our shared “notions of justice.” Full disclosure will also help the Court
22 ensure that the Government fulfills its statutory obligation under 18 U.S.C. § 2255
23 (providing civil remedies for the minor victims of pornography offenses) to make
24 restitution to all known victims whose images were posted and distributed by the FBI
25 during the time it controlled and operated “Website A.”

1 **IV. CONCLUSION**

2 For the reasons stated above, the Court should grant the defense's
3 accompanying Motion to Compel Discovery; schedule a hearing to determine the true
4 extent of the harm caused by the Government's investigatory tactics; and dismiss the
5 indictment if the Court finds that the governmental conduct leading to the charges
6 against Mr. Michaud cannot be reconciled with fundamental expectations of decency
7 and fairness.

8 DATED this 20th day of November, 2015.

9 Respectfully submitted,

10 *s/ Colin Fieman*

11 *s/ Linda Sullivan*

12 Attorneys for Jay Michaud
13
14
15
16
17
18
19
20
21
22
23
24
25
26

CERTIFICATE OF SERVICE

I hereby certify that on the date shown below I e-filed with the Clerk of the Court the foregoing Motion and Memorandum in Support of Motion to Dismiss Indictment, Proposed Order, and Sealed Exhibit B. I used the CM/ECF system, which will send notification of this filing to the Assistant United States Attorneys registered as participants to this case.

DATED this 20th day of November, 2015.

s/Amy Strickling
Amy Strickling, Paralegal